

**UNIVERSIDAD ANDINA DEL CUSCO**  
**FACULTAD DE INGENIERÍA Y ARQUITECTURA**  
**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**



**TEMA**

**“FIREWALL”**

**DOCENTE**

Mgt. Ing. Ediwn Carrasco Poblete

**ALUMNOS**

Espinosa Alarcon, Brian

Montalico Castro, Frank

Puelles Uñurucu, Gabriel Yoshwa

Valle Ccorimanya, Jhon Darwin

CUSCO – PERÚ

2023

## **PRESENTACIÓN**

El presente trabajo es sobre el desarrollo de la guía Firewall realizado por los siguientes integrantes Brian Espinoza Alarcon, Frank Montalico Castro, Puelles Uñurucu, Gabriel Yoshwa, Valle Ccorimanya, Jhon Darwin, para el curso de Seguridad de Tecnologías de Información y Comunicación dirigido hacia el Ing. Edwin Carrasco Poblete de la Universidad Andina del Cusco con el propósito de conocer e implementar un firewall en una red local para un sistema operativo linux.

## **INTRODUCCIÓN**

La Seguridad en los sistemas y la red son esenciales para cualquier entorno informático. Una de las herramientas más importantes para lograr este propósito es la implementación de un firewall que es un sistema de seguridad que controla el tráfico de red entrante y saliente en el que filtra mediante reglas que se hayan establecido. En el presente trabajo nos centraremos en establecer las reglas establecidas por los criterios de calificación para establecer la comunicación de red entre firewall, intranet, internet y dmz.

## ÍNDICE GENERAL

<b>PRESENTACIÓN.....</b>	<b>1</b>
<b>INTRODUCCIÓN.....</b>	<b>2</b>
<b>ÍNDICE GENERAL.....</b>	<b>3</b>
<b>ÍNDICE DE FIGURAS.....</b>	<b>4</b>
<b>Marco Teórico.....</b>	<b>5</b>
IMPLEMENTACIÓN.....	6
FIREWALL.....	7
INTRANET.....	8
DMZ.....	10
INTERNET.....	23
EJERCICIOS PROPUESTOS.....	24
EJERCICIO 1.....	24
EJERCICIO 2.....	26
EJERCICIO 3.....	28
<b>CONCLUSIÓN.....</b>	<b>31</b>
<b>REFERENCIAS BIBLIOGRÁFICAS.....</b>	<b>32</b>

## **Marco Teórico**

### **Firewall**

Un firewall es un sistema de seguridad informática diseñado para proteger una red o un sistema informático de amenazas externas, filtrando el tráfico de red entrante y saliente según las reglas que se hayan establecido, y actuando como una barrera entre la red interna y el mundo exterior.

### **Internet**

Internet es una red mundial de computadoras interconectadas y dispositivos de red que utilizan un conjunto común de protocolos de comunicación para transmitir datos e información a través de la red. Internet se originó en la década de 1960 como una iniciativa de investigación del gobierno estadounidense para conectar computadoras y facilitar la comunicación entre investigadores en diferentes lugares. Hoy en día, Internet es una herramienta esencial para la comunicación, el comercio, el entretenimiento, la educación y muchos otros aspectos de la vida moderna.

### **DMZ**

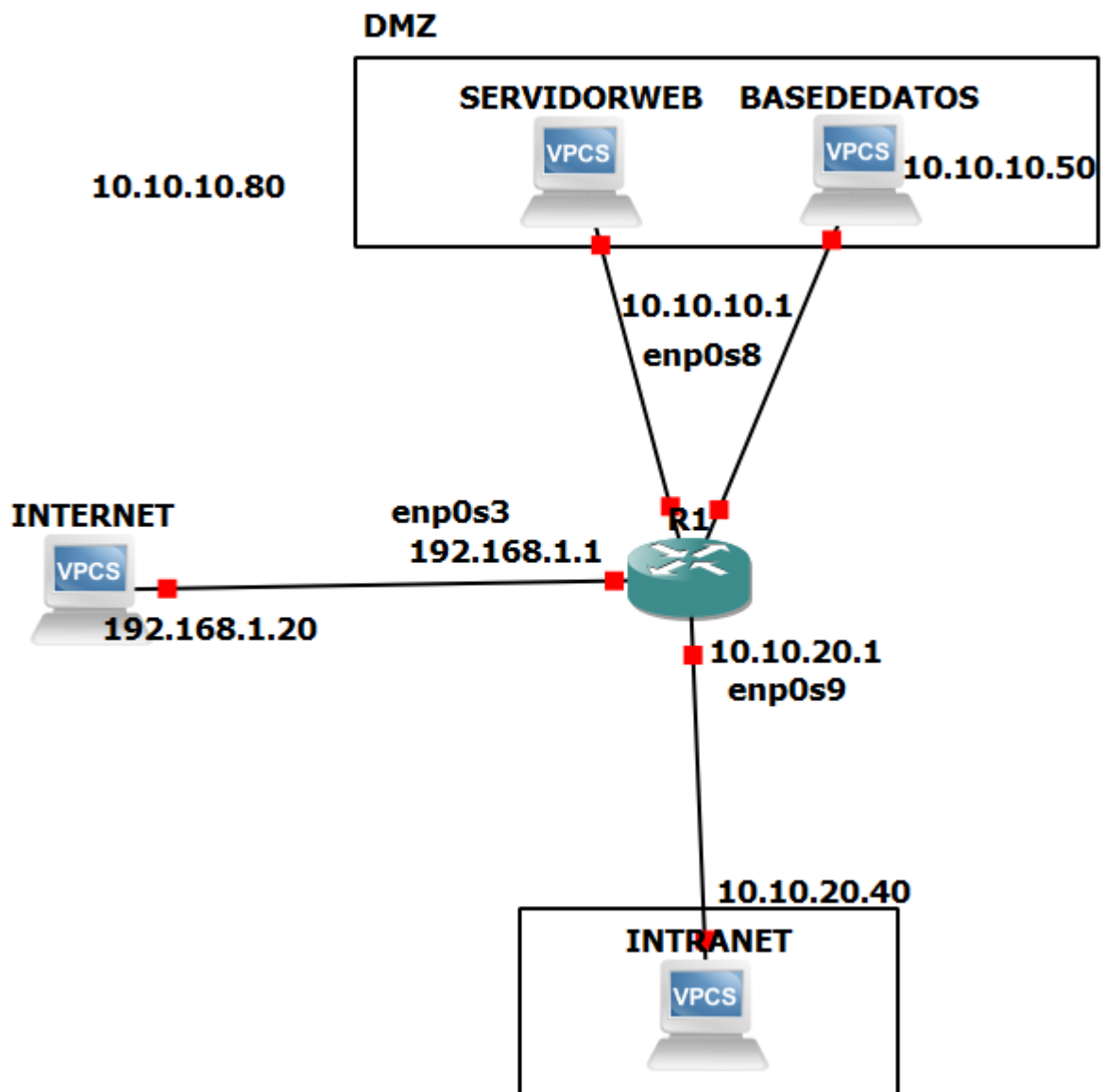
Es una red periférica que se encuentra entre una red interna protegida y una red externa no confiable, generalmente Internet. La DMZ se configura para proporcionar un nivel adicional de seguridad al aislar los servicios alojados en ella del resto de la red interna. Los sistemas ubicados en la DMZ suelen estar protegidos por firewalls y otras medidas de seguridad, y se permiten sólo los servicios y puertos necesarios para su correcto funcionamiento, mientras que se bloquean los accesos no autorizados.

### **Intranet**

La intranet es una red interna de una organización que utiliza tecnologías de Internet, como protocolos de comunicación y servicios web, para compartir información y recursos de manera segura y controlada dentro de la empresa. La intranet se diferencia de Internet en que es una red privada que está protegida por medidas de seguridad, como firewalls y sistemas de autenticación de usuarios, para restringir el acceso a la información y recursos a los empleados de la organización.

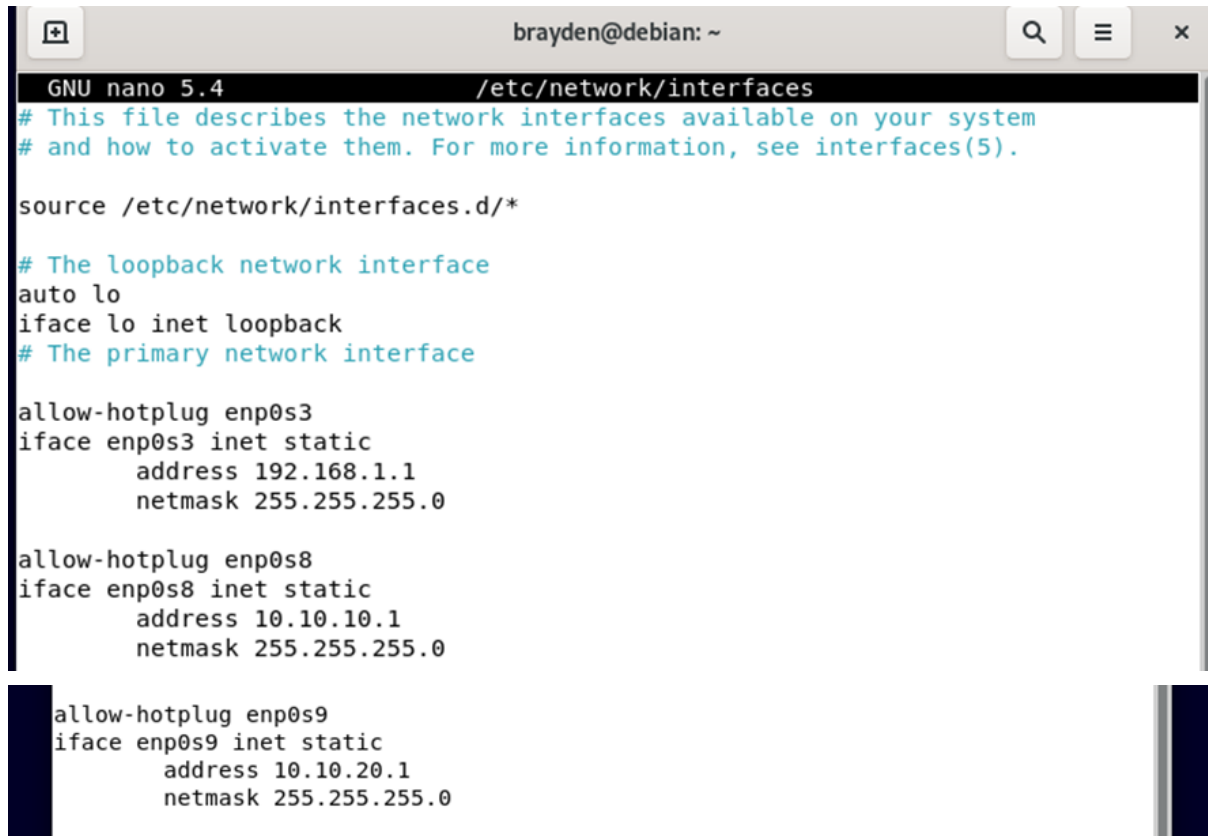
## IMPLEMENTACIÓN

Para comenzar con la implementación de la guía como primer paso diseñamos la topología de red del sistema



## FIREWALL

Configuramos las interfaces de redes en la FIREWALL accediendo al nano  
/etc/network/interfaces las cuales son enp0s3 = INTERNET, enp0s8 = DMZ, enp0s9 = RED  
LOCAL(INTRANET)



```
brayden@debian: ~
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface

allow-hotplug enp0s3
iface enp0s3 inet static
    address 192.168.1.1
    netmask 255.255.255.0

allow-hotplug enp0s8
iface enp0s8 inet static
    address 10.10.10.1
    netmask 255.255.255.0

allow-hotplug enp0s9
iface enp0s9 inet static
    address 10.10.20.1
    netmask 255.255.255.0
```

Luego Hacemos un listado de las tablas de iptables en el root despues de configurar la interfaz de red, con el comando IPTABLES -L y como podemos observar todos las políticas están ACCEPT

```
root@debian:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@debian:~#
```

Introducimos el comando para enrutar las ips:

```
root@debian:~# echo "1" > /proc/sys/net/ipv4/ip_forward
```

COMANDOS DE IPTABLES PARA ALGUNAS POLÍTICAS QUE REQUIERE EL  
DOCENTE

BLOQUEAR INTRANET A DMZ

```
root@debian:~# iptables -A FORWARD -i enp0s9 -o enp0s8 -p tcp --dport 3306 -m state --state NEW,ESTABLISHED -j DROP
```

bloquear internet a dmz

```
root@debian:~# iptables -A FORWARD -i enp0s3 -o enp0s8 -p tcp --dport 3306 -m state --state NEW,ESTABLISHED -j DROP
```

Los equipos de Intranet, no deben acceder al servidor web en DMZ.

```
root@debian:~# iptables -A FORWARD -i enp0s9 -o enp0s8 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j DROP
```

Los equipos de Intranet pueden salir a Internet, pero solo a servidores web (HTTP, HTTPS), no así a otros servicios como FTP, DNS o redes sociales como Facebook o redes P2P.

```
root@debian:~# iptables -A FORWARD -i enp0s9 -o enp0s3 -p tcp --dport 21 -m state --state NEW,ESTABLISHED -j DROP
root@debian:~# iptables -A FORWARD -i enp0s9 -o enp0s3 -p tcp --dport 49152:65535 -m state --state NEW,ESTABLISHED -j DROP
```

No se permiten conexiones SSH de Internet a Intranet, pero sí de Internet a DMZ y de Intranet a DMZ

```
root@debian:~# iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j DROP
```

Si deseamos bloquear el ping de internet, dmz o intranet la siguiente política

```
root@debian:~# iptables -A FORWARD -i enp0s9 -d 192.168.1.20 -j DROP
```



Al final listamos iptables -L

```
brayden@debian: ~  
root@debian:~# iptables -L  
Chain INPUT (policy ACCEPT)  
target      prot opt source                destination  
  
Chain FORWARD (policy ACCEPT)  
target      prot opt source                destination  
DROP        tcp  --  anywhere              anywhere            tcp dpt:mysql state  
NEW,ESTABLISHED  
DROP        tcp  --  anywhere              anywhere            tcp dpt:mysql state  
NEW,ESTABLISHED  
DROP        tcp  --  anywhere              anywhere            tcp dpt:http state  
NEW,ESTABLISHED  
DROP        tcp  --  anywhere              anywhere            tcp dpt:ftp state  
NEW,ESTABLISHED  
DROP        tcp  --  anywhere              anywhere            tcp dpt:smtp state  
NEW,ESTABLISHED  
DROP        tcp  --  anywhere              anywhere            tcp dpt:ssh state  
NEW,ESTABLISHED  
  
Chain OUTPUT (policy ACCEPT)  
target      prot_opt source                destination
```

Para guardar las políticas hechas en el iptables ponemos el siguiente comando:

```
root@debian:~# iptables-save > /home/iptables.v4
```

Para recuperar la copia de seguridad de iptables, cuando volvamos a prender la FIREWALL utilizamos este comando

```
brayden@debian: ~  
root@debian:~# iptables-restore < /home/iptables.v4
```

## INTRANET

Como primer paso asignamos la ip correspondiente a la topología para Intranet 10.10.20.40  
Asignación de ip:

Cancel **Wired connection 1** Apply

Details Identity **IPv4** IPv6 Security

**IPv4 Method**

☐ Automatic (DHCP) ☐ Link-Local Only

☒ Manual ☐ Disable

☐ Shared to other computers

**Addresses**

Address	Netmask	Gateway	
10.10.20.40	255.255.255.0	10.10.20.1	✕
			✕

**DNS** Automatic ☒

Separate IP addresses with commas

Intranet tiene ping hacia Internet

```
root@debian:~# ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=63 time=3.42 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=63 time=11.1 ms
```

Intranet tiene ping hacia Dmz página web

```
root@debian:~# ping 10.10.10.80
PING 10.10.10.80 (10.10.10.80) 56(84) bytes of data.
64 bytes from 10.10.10.80: icmp_seq=1 ttl=63 time=33.7 ms
64 bytes from 10.10.10.80: icmp_seq=2 ttl=63 time=4.50 ms
64 bytes from 10.10.10.80: icmp_seq=3 ttl=63 time=3.83 ms
```

Intranet tiene ping hacia DMZ base de datos

```
root@debian:~# ping 10.10.10.50
PING 10.10.10.50 (10.10.10.50) 56(84) bytes of data.
64 bytes from 10.10.10.50: icmp_seq=1 ttl=63 time=7.88 ms
64 bytes from 10.10.10.50: icmp_seq=2 ttl=63 time=4.00 ms
```

Instalación del SSH

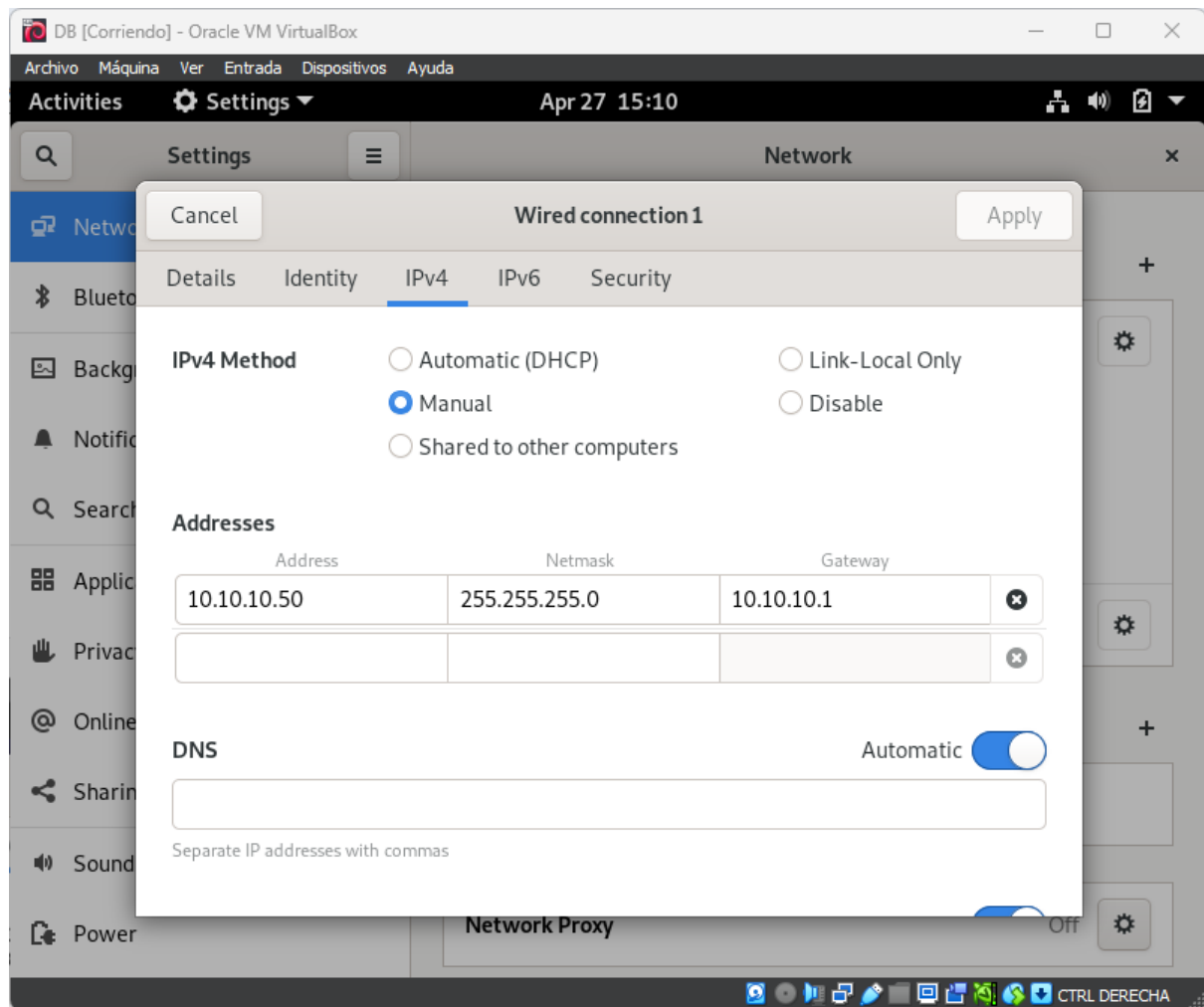
Para una conexión con ssh instalamos el ssh en intranet

```
fmc@debian: ~  
root@debian:~# apt install openssh-server  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  openssh-sftp-server runit-helper  
Suggested packages:  
  molly-guard monkeysphere ssh-askpass ufw  
The following NEW packages will be installed:  
  openssh-server openssh-sftp-server runit-helper  
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.  
Need to get 446 kB of archives.  
After this operation, 1,765 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://deb.debian.org/debian bullseye/main amd64 openssh-sftp-server amd64 1:8.4p1-5+deb11u1 [52.4 kB]  
Get:2 http://deb.debian.org/debian bullseye/main amd64 runit-helper all 2.10.3 [7,808 B]  
Get:3 http://deb.debian.org/debian bullseye/main amd64 openssh-server amd64 1:8.4p1-5+deb11u1 [385 kB]  
Fetched 446 kB in 1s (637 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package openssh-sftp-server.  
(Reading database ... 141356 files and directories currently installed.)  
root@debian:~# ssh -V  
OpenSSH_8.4p1 Debian-5+deb11u1, OpenSSL 1.1.1n 15 Mar 2022  
root@debian:~#
```

## DMZ

## BASE DE DATOS

Asignación de ip, mascara y gateway de la DB



DB hace ping hacia el web, intranet y internet

The image shows a screenshot of a VirtualBox window titled "DB [Corriendo] - Oracle VM VirtualBox". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". Below the menu bar is a toolbar with "Activities" and "Terminal". The main area displays a terminal window titled "vboxuser@Linux: ~". The terminal shows the following output:

```
root@Linux:~# ping 10.10.10.80
PING 10.10.10.80 (10.10.10.80) 56(84) bytes of data.
64 bytes from 10.10.10.80: icmp_seq=1 ttl=64 time=1.36 ms
64 bytes from 10.10.10.80: icmp_seq=2 ttl=64 time=0.899 ms
^C
--- 10.10.10.80 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 0.899/1.129/1.359/0.230 ms
root@Linux:~# ping 10.10.20.40
PING 10.10.20.40 (10.10.20.40) 56(84) bytes of data.
64 bytes from 10.10.20.40: icmp_seq=1 ttl=63 time=4.18 ms
64 bytes from 10.10.20.40: icmp_seq=2 ttl=63 time=4.08 ms
^C
--- 10.10.20.40 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1055ms
rtt min/avg/max/mdev = 4.075/4.128/4.181/0.053 ms
root@Linux:~# ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=63 time=6.43 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=63 time=3.35 ms
^C
--- 192.168.1.20 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1039ms
rtt min/avg/max/mdev = 3.350/4.887/6.425/1.537 ms
root@Linux:~#
```

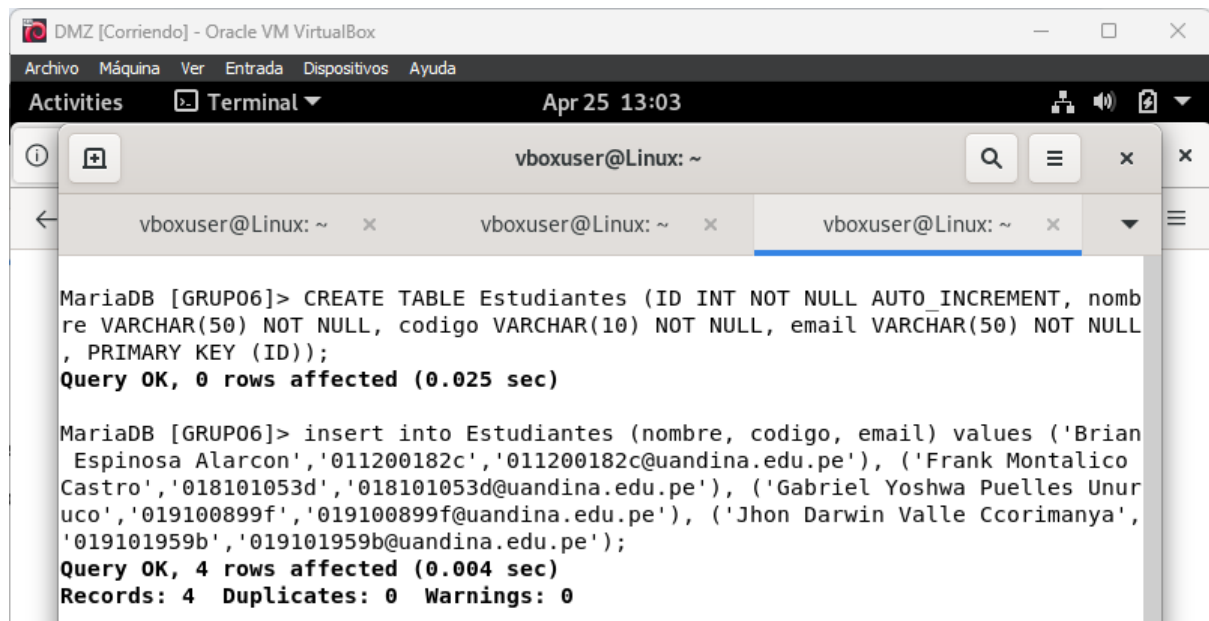
The terminal window has a search bar and a menu icon in the top right corner. The bottom of the window shows a taskbar with various icons and the text "CTRL DERECHA".

Instalación de mariadb

The screenshot shows a terminal window titled "vboxuser@Linux: ~" within an Oracle VM VirtualBox environment. The terminal output shows the command `sudo apt install mariadb-server` being executed. The output lists various additional packages to be installed, suggested packages, and new packages to be installed, along with disk space requirements.

```
root@Linux:~# sudo apt install mariadb-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  galera-4 gawk libaio1 libcgi-fast-perl libcgi-pm-perl
  libconfig-inifiles-perl libdbd-mariadb-perl libdbi-perl libfcgi-bin
  libfcgi-perl libfcgi0ldbl libhtml-template-perl libmariadb3 libsigsegv2
  libterm-readkey-perl mariadb-client-10.5 mariadb-client-core-10.5
  mariadb-common mariadb-server-10.5 mariadb-server-core-10.5 mysql-common
  rsync socat
Suggested packages:
  gawk-doc libmldbm-perl libnet-daemon-perl libsql-statement-perl
  libipc-sharedcache-perl mailx mariadb-test netcat-openbsd openssh-server
The following NEW packages will be installed:
  galera-4 gawk libaio1 libcgi-fast-perl libcgi-pm-perl
  libconfig-inifiles-perl libdbd-mariadb-perl libdbi-perl libfcgi-bin
  libfcgi-perl libfcgi0ldbl libhtml-template-perl libmariadb3 libsigsegv2
  libterm-readkey-perl mariadb-client-10.5 mariadb-client-core-10.5
  mariadb-common mariadb-server mariadb-server-10.5 mariadb-server-core-10.5
  mysql-common rsync socat
0 upgraded, 24 newly installed, 0 to remove and 0 not upgraded.
Need to get 17.2 MB of archives.
After this operation, 158 MB of additional disk space will be used.
```

Creación de la base de datos, tablas y introducir datos



The screenshot shows a terminal window titled "vboxuser@Linux: ~" within an Oracle VM VirtualBox environment. The terminal displays two SQL commands and their results:

```
MariaDB [GRUP06]> CREATE TABLE Estudiantes (ID INT NOT NULL AUTO INCREMENT, nombre VARCHAR(50) NOT NULL, codigo VARCHAR(10) NOT NULL, email VARCHAR(50) NOT NULL, PRIMARY KEY (ID));
Query OK, 0 rows affected (0.025 sec)

MariaDB [GRUP06]> insert into Estudiantes (nombre, codigo, email) values ('Brian Espinosa Alarcon','011200182c','011200182c@uandina.edu.pe'), ('Frank Montalico Castro','018101053d','018101053d@uandina.edu.pe'), ('Gabriel Yoshwa Puelles Unur uco','019100899f','019100899f@uandina.edu.pe'), ('Jhon Darwin Valle Ccorimanya','019101959b','019101959b@uandina.edu.pe');
Query OK, 4 rows affected (0.004 sec)
Records: 4 Duplicates: 0 Warnings: 0
```

Mostrar la tabla creada junto a los datos introducidos

```

MariaDB [(none)]> use GRUP06
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [GRUP06]> show tables;
+-----+
| Tables_in_GRUP06 |
+-----+
| Estudiantes      |
+-----+
1 row in set (0.001 sec)

MariaDB [GRUP06]> select*from Estudiantes;
+-----+-----+-----+-----+
| ID | nombre                                     | codigo   | email                                     |
+-----+-----+-----+-----+
| 1  | Brian Espinosa Alarcon                   | 011200182c | 011200182c@uandina.edu.pe |
| 2  | Frank Montalico Castro                   | 018101053d | 018101053d@uandina.edu.pe |
| 3  | Gabriel Yoshwa Puelles Unuruco          | 019100899f | 019100899f@uandina.edu.pe |
| 4  | Jhon Darwin Valle Ccorimanya            | 019101959b | 019101959b@uandina.edu.pe |
+-----+-----+-----+-----+
4 rows in set (0.001 sec)

```

Configuración para el permiso de acceso a todas las direcciones IP

```

GNU nano 5.4 /etc/mysql/mariadb.conf.d/50-server.cnf

# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 0.0.0.0

#
# * Fine Tuning
#

#key_buffer_size        = 128M
#max_allowed_packet     = 1G
#thread_stack           = 192K
#thread_cache_size      = 8
# This replaces the startup script and checks MyISAM tables if needed
# the first time they are touched
#myisam_recover_options = BACKUP
#max_connections        = 100
#table_cache            = 64

[ Wrote 117 lines ]

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line

```



Creación del usuario con privilegios y mostrarlo en la tabla para el mariadb cliente

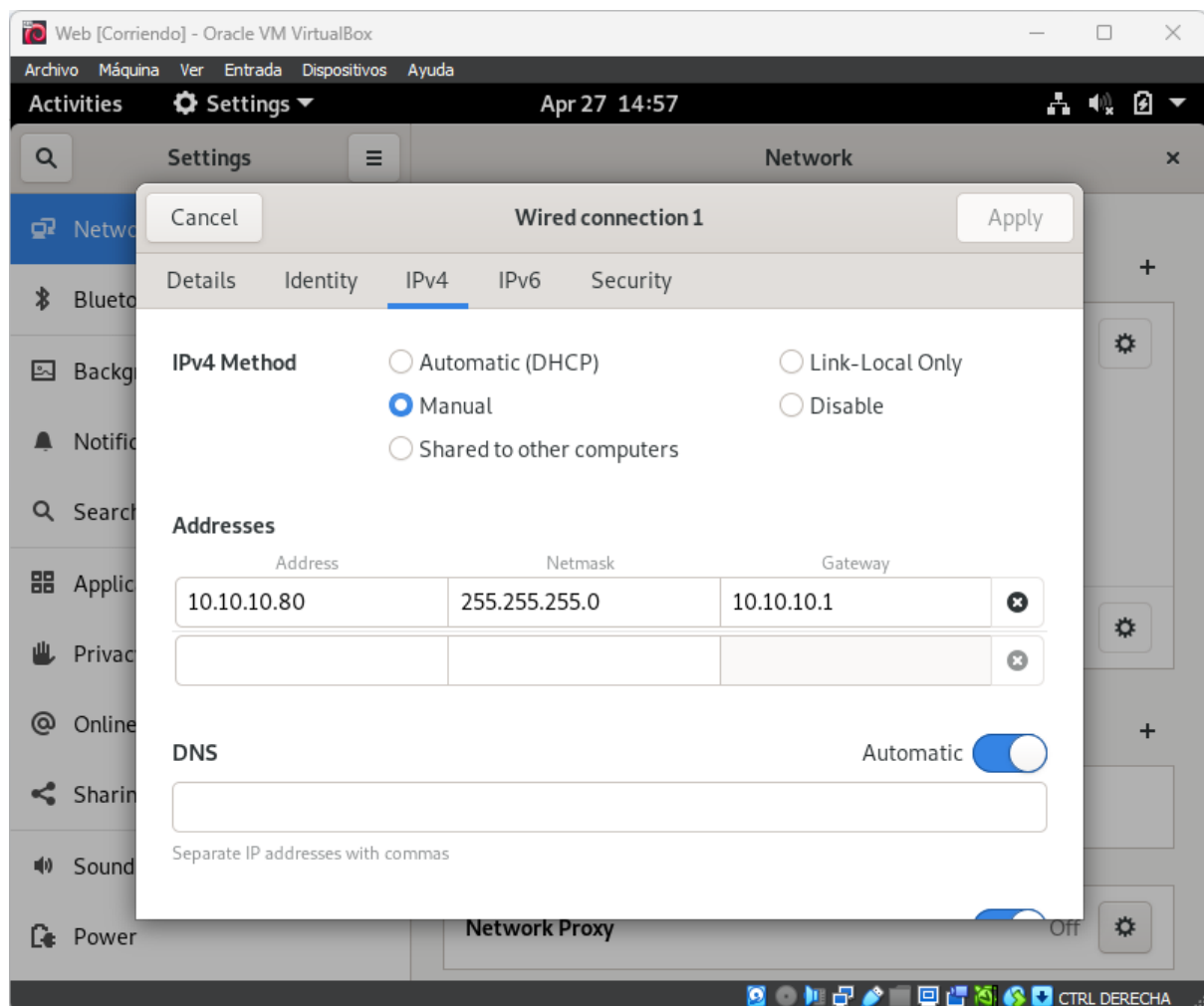
```
MariaDB [(none)]> CREATE USER 'Cliente'@'%' IDENTIFIED BY '123';
Query OK, 0 rows affected (0.006 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON *.* TO 'Cliente'@'%';
Query OK, 0 rows affected (0.002 sec)

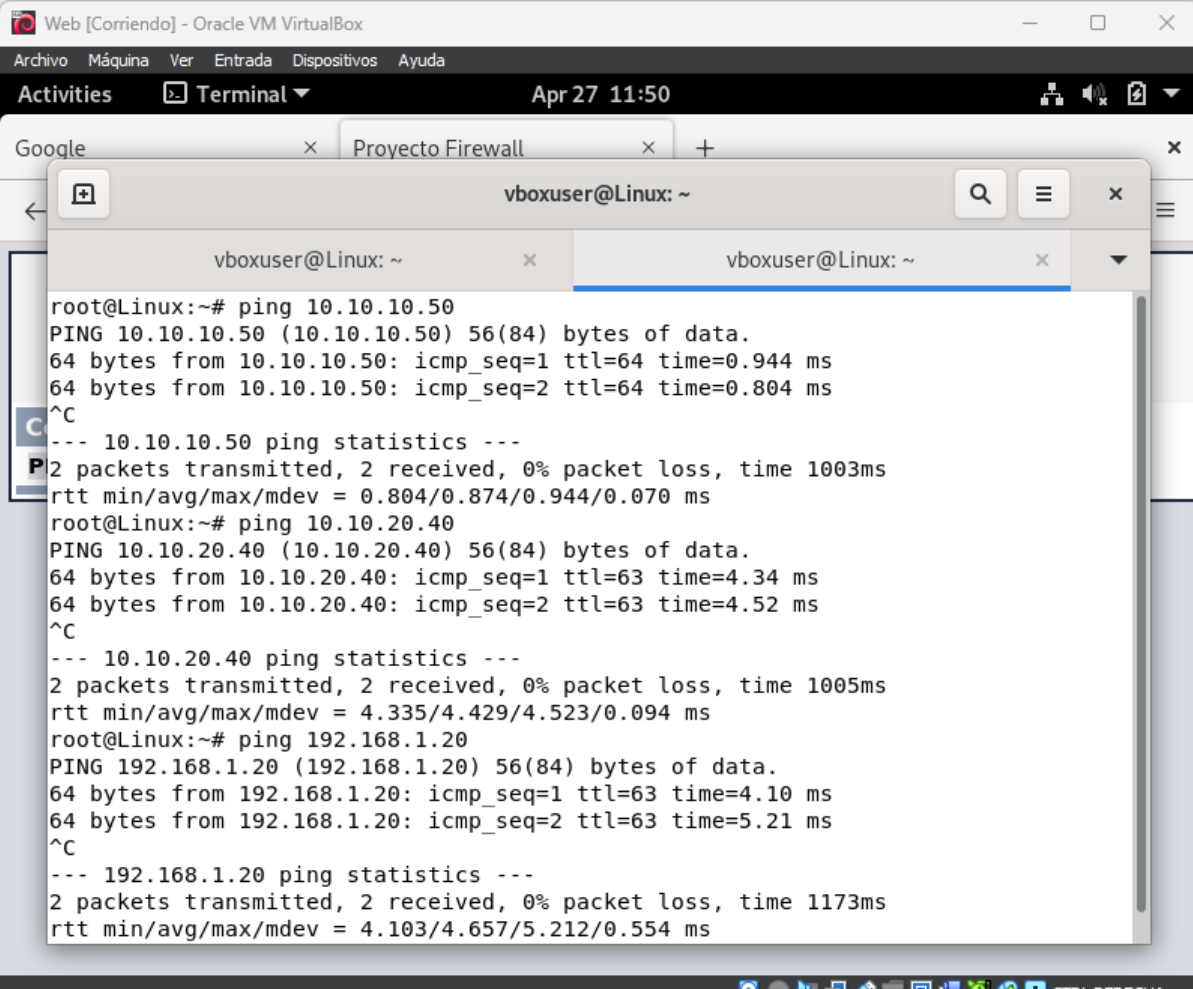
MariaDB [(none)]> Select User, Host from mysql.user;
+-----+-----+
| User      | Host      |
+-----+-----+
| Cliente   | %         |
| mariadb.sys | localhost |
| mysql     | localhost |
| root      | localhost |
+-----+-----+
```

## WEB

Asignación de ip, mascara y gateway de la Web



Web hace ping hacia el BD, intranet y internet

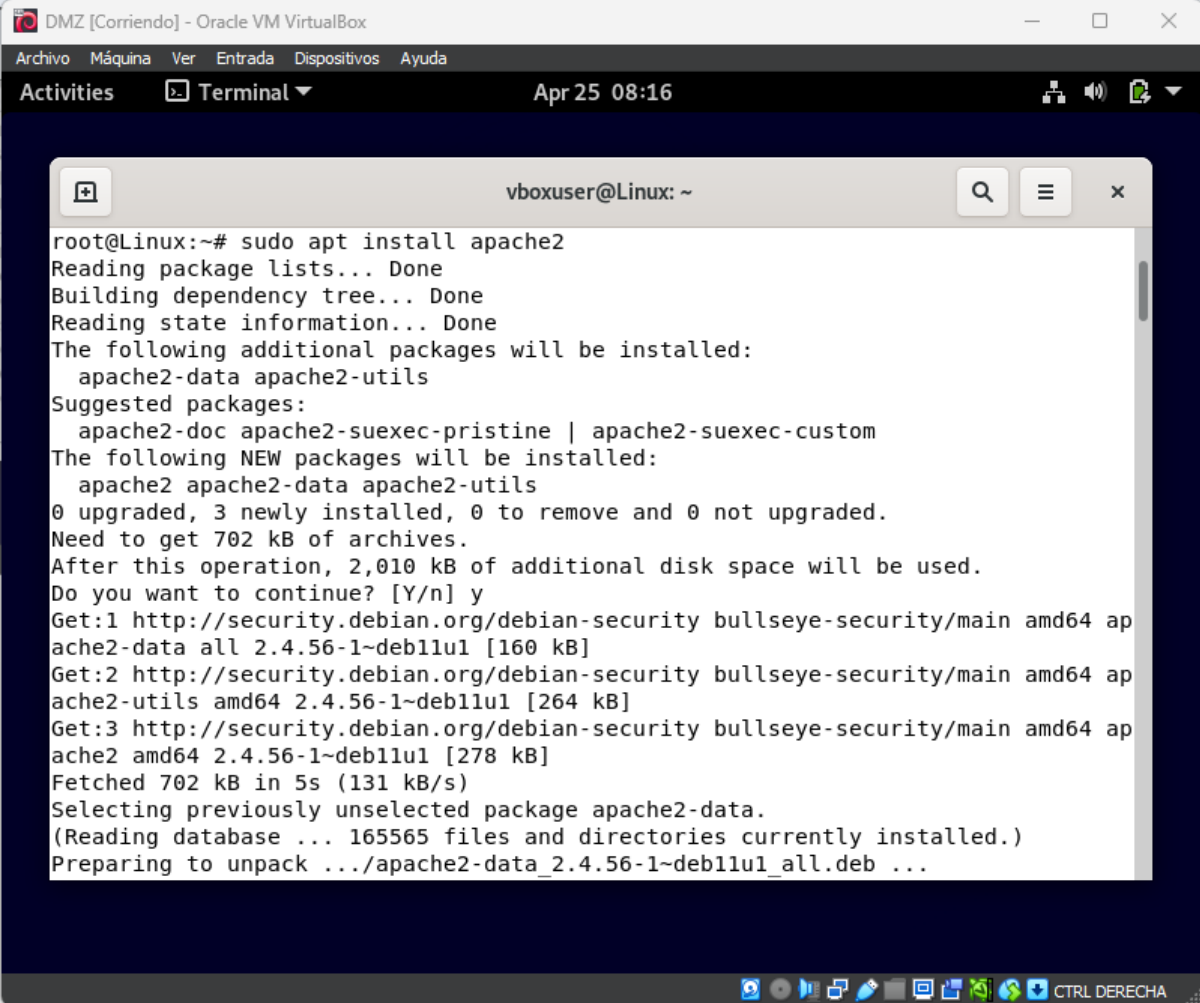


The screenshot shows a Linux terminal window titled "vboxuser@Linux: ~" with a search bar and window controls. The terminal output shows the following commands and results:

```
root@Linux:~# ping 10.10.10.50
PING 10.10.10.50 (10.10.10.50) 56(84) bytes of data.
64 bytes from 10.10.10.50: icmp_seq=1 ttl=64 time=0.944 ms
64 bytes from 10.10.10.50: icmp_seq=2 ttl=64 time=0.804 ms
^C
--- 10.10.10.50 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 0.804/0.874/0.944/0.070 ms
root@Linux:~# ping 10.10.20.40
PING 10.10.20.40 (10.10.20.40) 56(84) bytes of data.
64 bytes from 10.10.20.40: icmp_seq=1 ttl=63 time=4.34 ms
64 bytes from 10.10.20.40: icmp_seq=2 ttl=63 time=4.52 ms
^C
--- 10.10.20.40 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 4.335/4.429/4.523/0.094 ms
root@Linux:~# ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=63 time=4.10 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=63 time=5.21 ms
^C
--- 192.168.1.20 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1173ms
rtt min/avg/max/mdev = 4.103/4.657/5.212/0.554 ms
```

The terminal window is part of a larger application window titled "Web [Corriendo] - Oracle VM VirtualBox". The background shows a web browser with tabs for "Google" and "Proyecto Firewall". The system clock at the top right indicates "Apr 27 11:50". The bottom of the screen shows a taskbar with various icons and the text "CTRL DERECHA".

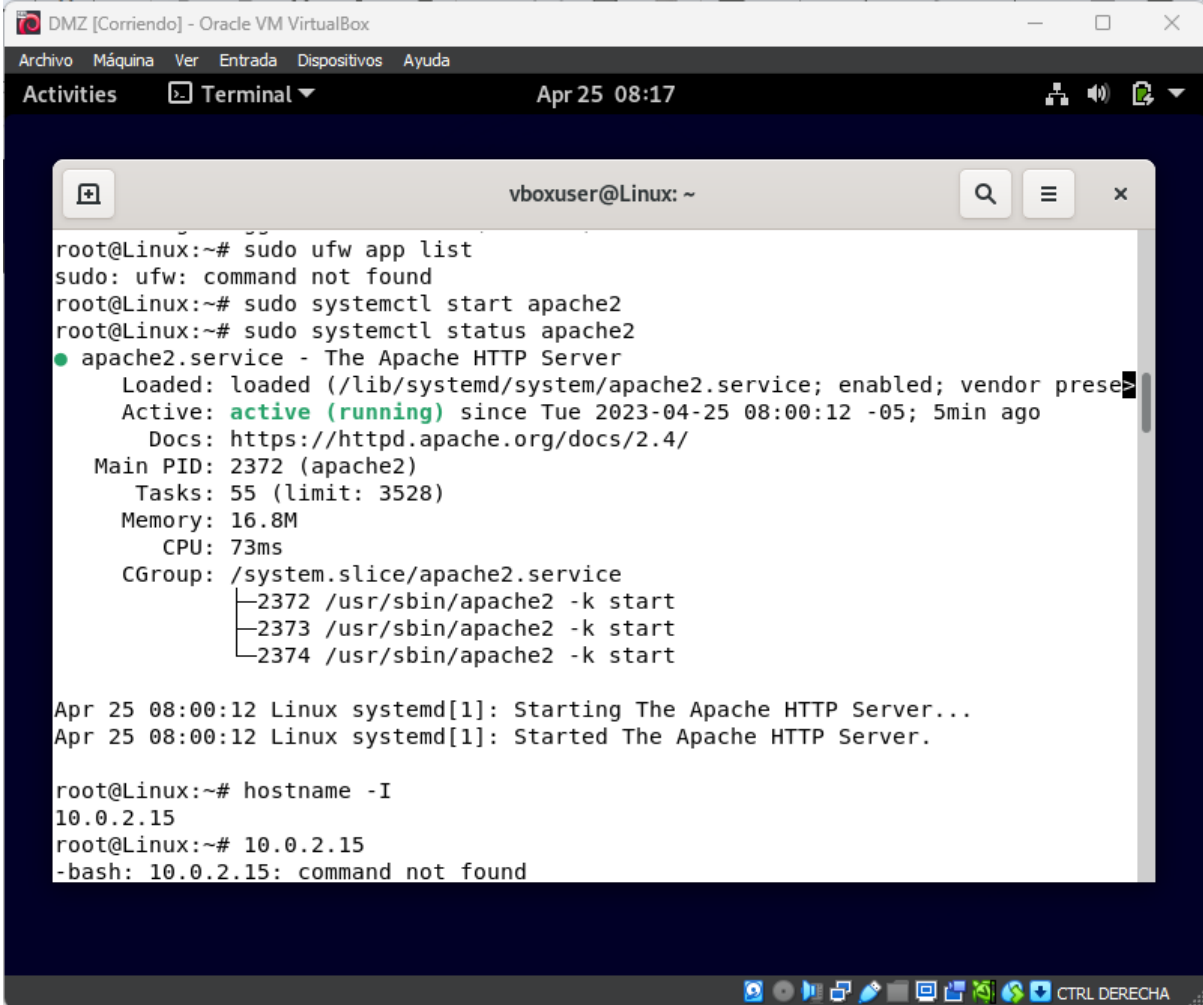
## Instalación de Apache2



The screenshot shows a terminal window titled "vboxuser@Linux: ~" within an Oracle VM VirtualBox environment. The terminal output shows the command `sudo apt install apache2` being executed. The system reports that it will install `apache2-data` and `apache2-utils` along with `apache2`. It also shows the progress of downloading these packages from the Debian security repository.

```
root@Linux:~# sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-data apache2-utils
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-data apache2-utils
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 702 kB of archives.
After this operation, 2,010 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://security.debian.org/debian-security bullseye-security/main amd64 ap
ache2-data all 2.4.56-1-deb11u1 [160 kB]
Get:2 http://security.debian.org/debian-security bullseye-security/main amd64 ap
ache2-utils amd64 2.4.56-1-deb11u1 [264 kB]
Get:3 http://security.debian.org/debian-security bullseye-security/main amd64 ap
ache2 amd64 2.4.56-1-deb11u1 [278 kB]
Fetched 702 kB in 5s (131 kB/s)
Selecting previously unselected package apache2-data.
(Reading database ... 165565 files and directories currently installed.)
Preparing to unpack .../apache2-data_2.4.56-1-deb11u1_all.deb ...
```

Iniciar y mostrar el estado actual del servicio del servidor web Apache.



The screenshot shows a terminal window titled "vboxuser@Linux: ~" within an Oracle VM VirtualBox environment. The terminal output shows the following commands and their results:

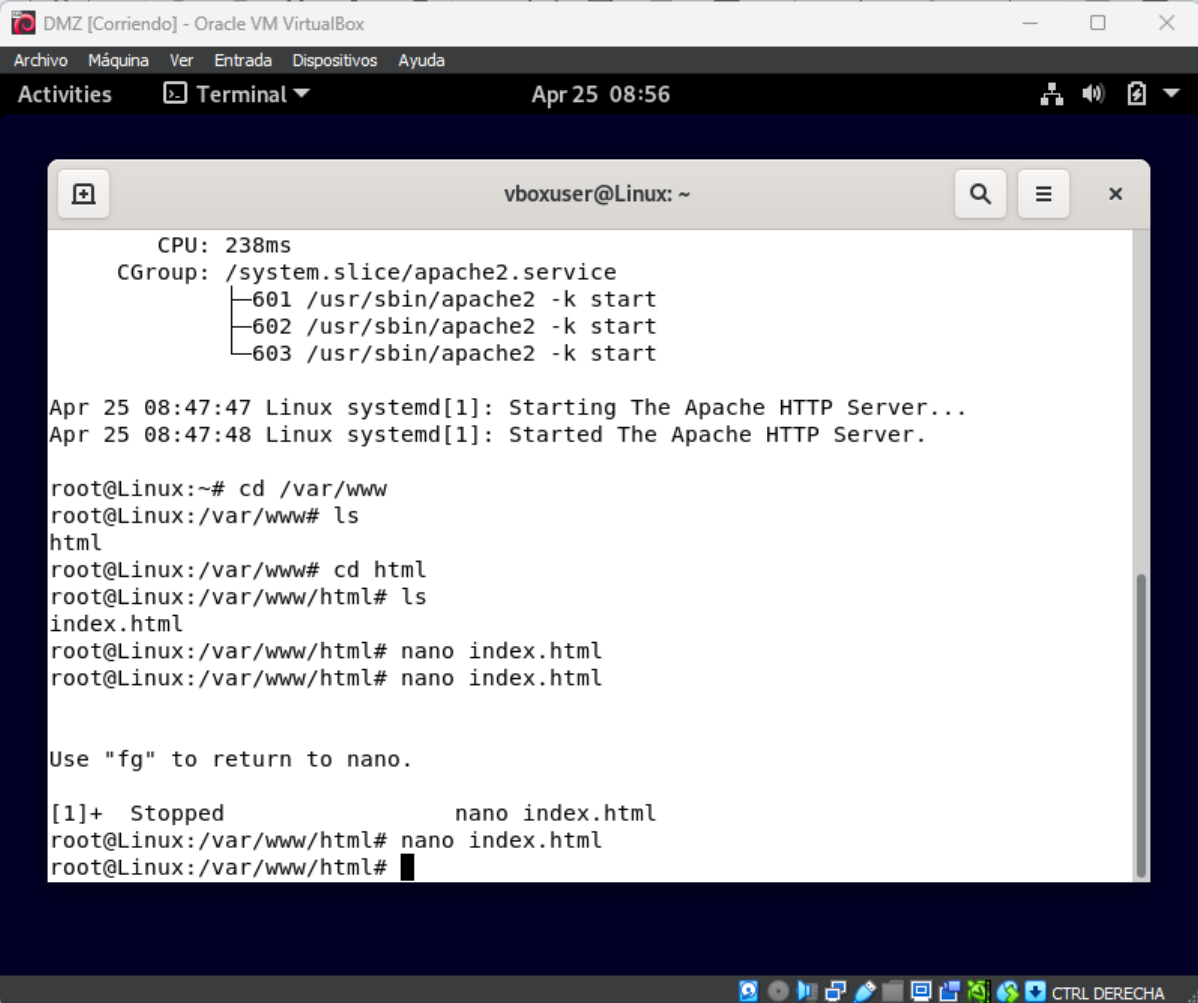
```
root@Linux:~# sudo ufw app list
sudo: ufw: command not found
root@Linux:~# sudo systemctl start apache2
root@Linux:~# sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese>
   Active: active (running) since Tue 2023-04-25 08:00:12 -05; 5min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2372 (apache2)
     Tasks: 55 (limit: 3528)
    Memory: 16.8M
       CPU: 73ms
    CGroup: /system.slice/apache2.service
            └─2372 /usr/sbin/apache2 -k start
              └─2373 /usr/sbin/apache2 -k start
                └─2374 /usr/sbin/apache2 -k start

Apr 25 08:00:12 Linux systemd[1]: Starting The Apache HTTP Server...
Apr 25 08:00:12 Linux systemd[1]: Started The Apache HTTP Server.

root@Linux:~# hostname -I
10.0.2.15
root@Linux:~# 10.0.2.15
-bash: 10.0.2.15: command not found
```

The terminal window is part of a desktop environment with a top bar showing "Activities", "Terminal", and the date/time "Apr 25 08:17". The bottom of the window shows a taskbar with various application icons and a "CTRL DERECHA" label.

Ingresar a configurar la página WEB



The screenshot shows a terminal window titled "vboxuser@Linux: ~" within a VirtualBox environment. The terminal displays the following commands and output:

```
CPU: 238ms
CGroup: /system.slice/apache2.service
├─601 /usr/sbin/apache2 -k start
├─602 /usr/sbin/apache2 -k start
└─603 /usr/sbin/apache2 -k start

Apr 25 08:47:47 Linux systemd[1]: Starting The Apache HTTP Server...
Apr 25 08:47:48 Linux systemd[1]: Started The Apache HTTP Server.

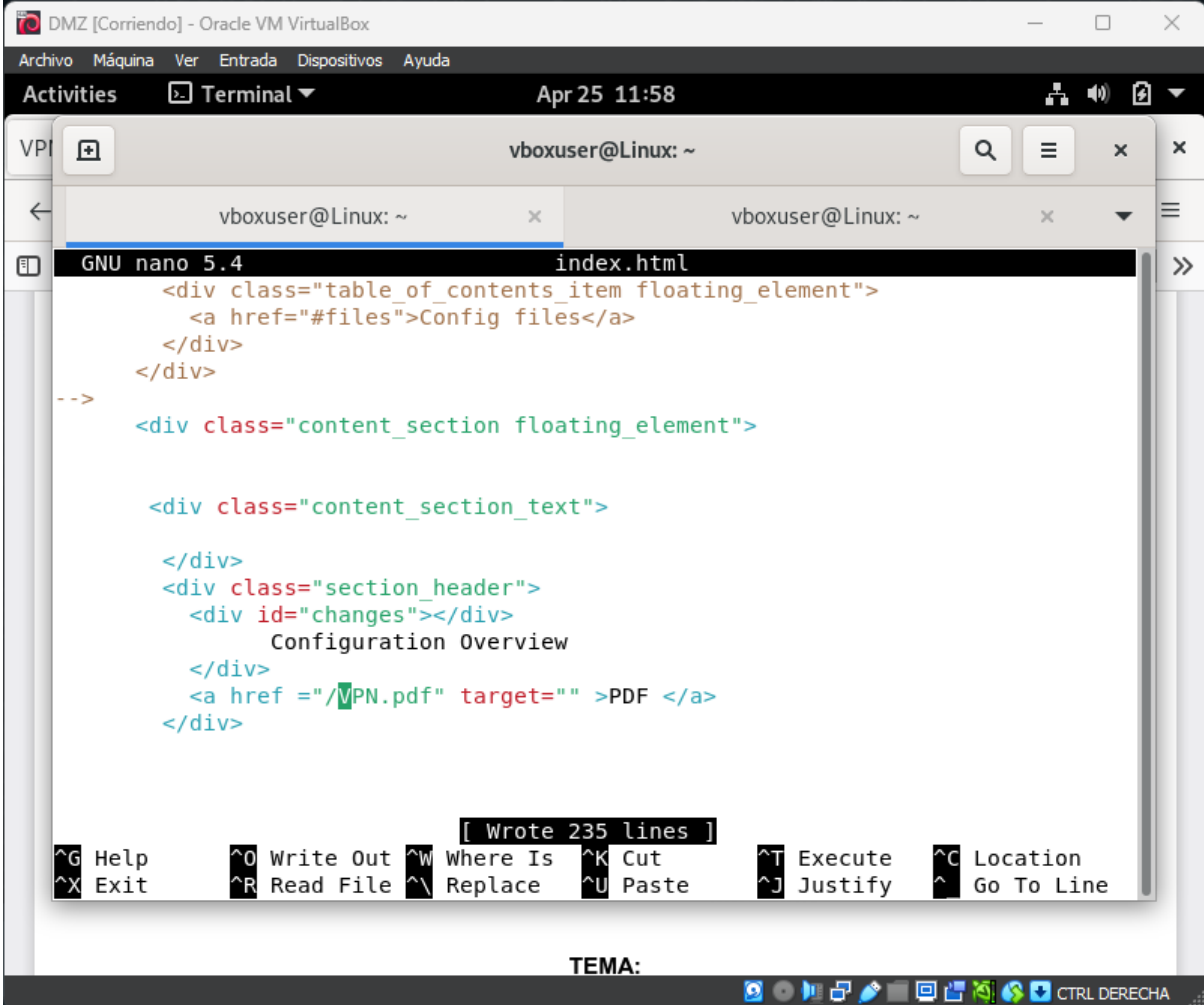
root@Linux:~# cd /var/www
root@Linux:/var/www# ls
html
root@Linux:/var/www# cd html
root@Linux:/var/www/html# ls
index.html
root@Linux:/var/www/html# nano index.html
root@Linux:/var/www/html# nano index.html

Use "fg" to return to nano.

[1]+  Stopped                  nano index.html
root@Linux:/var/www/html# nano index.html
root@Linux:/var/www/html#
```

The terminal window is part of a larger interface with a menu bar (Archivo, Máquina, Ver, Entrada, Dispositivos, Ayuda) and a status bar (Activities, Terminal, Apr 25 08:56). The bottom of the window shows a taskbar with various application icons and a "CTRL DERECHA" label.

## Configuración de la Web y enlazar el informe pdf



The screenshot shows a VirtualBox window titled "DMZ [Corriendo] - Oracle VM VirtualBox". Inside, a terminal window is open with the prompt "vboxuser@Linux: ~". The terminal displays the GNU nano 5.4 editor editing a file named "index.html". The code in the editor is as follows:

```
index.html
<div class="table_of_contents_item floating_element">
  <a href="#files">Config files</a>
</div>
-->
<div class="content_section floating_element">

  <div class="content_section_text">

    </div>
    <div class="section_header">
      <div id="changes"></div>
      Configuration Overview
    </div>
    <a href ="/VPN.pdf" target="" >PDF </a>
  </div>
```

At the bottom of the terminal window, a status bar indicates "[ Wrote 235 lines ]". Below the status bar, a list of keyboard shortcuts is displayed:

^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute	^C Location
^X Exit	^R Read File	^_ Replace	^U Paste	^J Justify	^_ Go To Line

At the very bottom of the terminal window, the word "TEMA:" is visible. The bottom of the VirtualBox window shows a taskbar with various icons and the text "CTRL DERECHA".

## Instalación del SSH para la DB y la Web

```
root@Linux:~# sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  openssh-sftp-server runit-helper
Suggested packages:
  molly-guard monkeysphere ssh-askpass ufw
The following NEW packages will be installed:
  openssh-server openssh-sftp-server runit-helper
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 446 kB of archives.
After this operation, 1,765 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bullseye/main amd64 openssh-sftp-server amd64
  1:8.4p1-5+deb11u1 [52.4 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 runit-helper all 2.10.3 [
  7.808 B]
```

## Iniciar el servicio de SSH tanto en DB y en Web

```
root@Linux:~# sudo service ssh start
root@Linux:~# █
```

## INTERNET

### Asignación de IP



### Ping hacia Intranet

```
root@internet:/home/servidorweb# ping 10.10.20.40
PING 10.10.20.40 (10.10.20.40) 56(84) bytes of data.
64 bytes from 10.10.20.40: icmp_seq=1 ttl=63 time=4.23 ms
64 bytes from 10.10.20.40: icmp_seq=2 ttl=63 time=4.47 ms
64 bytes from 10.10.20.40: icmp_seq=3 ttl=63 time=4.91 ms
```

### Ping hacia la BD

```
root@internet:/home/servidorweb# ping 10.10.10.50
PING 10.10.10.50 (10.10.10.50) 56(84) bytes of data.
64 bytes from 10.10.10.50: icmp_seq=1 ttl=63 time=4.86 ms
64 bytes from 10.10.10.50: icmp_seq=2 ttl=63 time=4.49 ms
64 bytes from 10.10.10.50: icmp_seq=3 ttl=63 time=4.26 ms
```

### Ping hacia el Servidor web

```
root@internet:/home/servidorweb# ping 10.10.10.80
PING 10.10.10.80 (10.10.10.80) 56(84) bytes of data.
64 bytes from 10.10.10.80: icmp_seq=1 ttl=63 time=5.47 ms
64 bytes from 10.10.10.80: icmp_seq=2 ttl=63 time=6.21 ms
64 bytes from 10.10.10.80: icmp_seq=3 ttl=63 time=4.86 ms
```

Este apartado funcionara como un simulador del Internet



## EJERCICIOS PROPUESTOS

### EJERCICIO 1

1. El servidor BD no debe ser accesible ni desde Internet, ni desde Intranet; solo de la propia DMZ.

#### Acceso a DB antes del bloqueo

##### Conexión en Internet

```
root@internet:/home/servidorweb# mysql -u Cliente -p -h 10.10.10.50 GRUP06
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 56
Server version: 10.5.18-MariaDB-0+deb11u1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [GRUP06]> show tables;
+-----+
| Tables_in_GRUP06 |
+-----+
| Estudiantes      |
+-----+
1 row in set (0,005 sec)
```

##### Conexión en Intranet

```

root@debian:~# mariadb -u Cliente -p -h 10.10.10.50 GRUP06
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 58
Server version: 10.5.18-MariaDB-0+deb11u1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [GRUP06]> show tables;
+-----+
| Tables_in_GRUP06 |
+-----+
| Estudiantes      |
+-----+
1 row in set (0.005 sec)

```

## Firewall bloquea puerto 3306 a Intranet y a Internet

Política que bloquea Intranet a DMZ

```

root@debian:~# iptables -A FORWARD -i enp0s9 -o enp0s8 -p tcp --dport 3306 -m state --state NEW,ESTABLISHED -j DROP

```

Política que bloquea Internet a DMZ

```

root@debian:~# iptables -A FORWARD -i enp0s3 -o enp0s8 -p tcp --dport 3306 -m state --state NEW,ESTABLISHED -j DROP

```

Conexión bloqueada en Internet

```

servidorweb@internet: ~
root@internet:/home/servidorweb# mysql -u Cliente -p -h 10.10.10.50 GRUP06
Enter password:

ERROR 2002 (HY000): Can't connect to MySQL server on '10.10.10.50' (115)

```

Conexión bloqueada en Intranet

```

root@debian:~# mariadb -u Cliente -p -h 10.10.10.50 GRUP06
Enter password:
ERROR 2002 (HY000): Can't connect to MySQL server on '10.10.10.50' (115)
root@debian:~#

```

## EJERCICIO 2

### 2. Servicio web:

- a) Los equipos de Intranet, no deben acceder al servidor web en DMZ.

Acceso de intranet a página web del DMZ antes del bloqueo



Firewall bloquea al servicio web de DMZ hacia Intranet y no puede acceder

```
root@debian:~# iptables -A FORWARD -i enp0s9 -o enp0s8 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j DROP
```

Intranet no puede acceder a pagina web de DMZ



Hmm. We're having trouble finding that site.

We can't connect to the server at www.mype.com.pe.

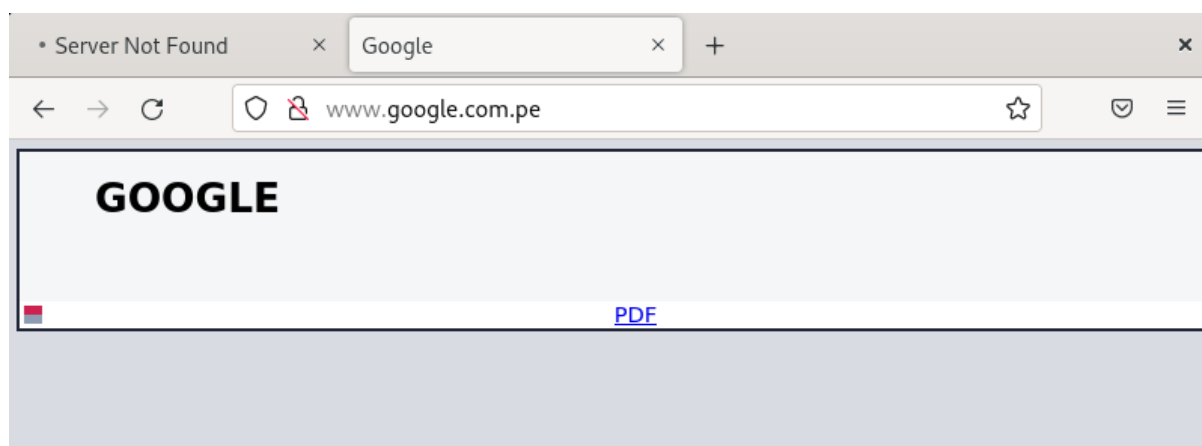
If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

Try Again

- b) Los equipos de Intranet pueden salir a Internet, pero solo a servidores web (HTTP, HTTPS), no así a otros servicios como FTP, DNS o redes sociales como Facebook o redes P2P.

Acceso de Intranet a Internet hacia su pagina web [www.google.com.pe](http://www.google.com.pe) ip: 192.168.1.20



POLÍTICAS QUE BLOQUEAN DNS,FTP, REDES SOCIALES ETC

```
root@debian:~# iptables -A FORWARD -i enp0s9 -o enp0s3 -p tcp --dport 21 -m state --state NEW,ESTABLISHED -j DROP
root@debian:~# iptables -A FORWARD -i enp0s9 -o enp0s3 -p tcp --dport 49152:65535 -m state --state NEW,ESTABLISHED -j DROP
```

### EJERCICIO 3

3. No se permiten conexiones SSH de Internet a Intranet, pero sí de Internet a DMZ y de Intranet a DMZ.

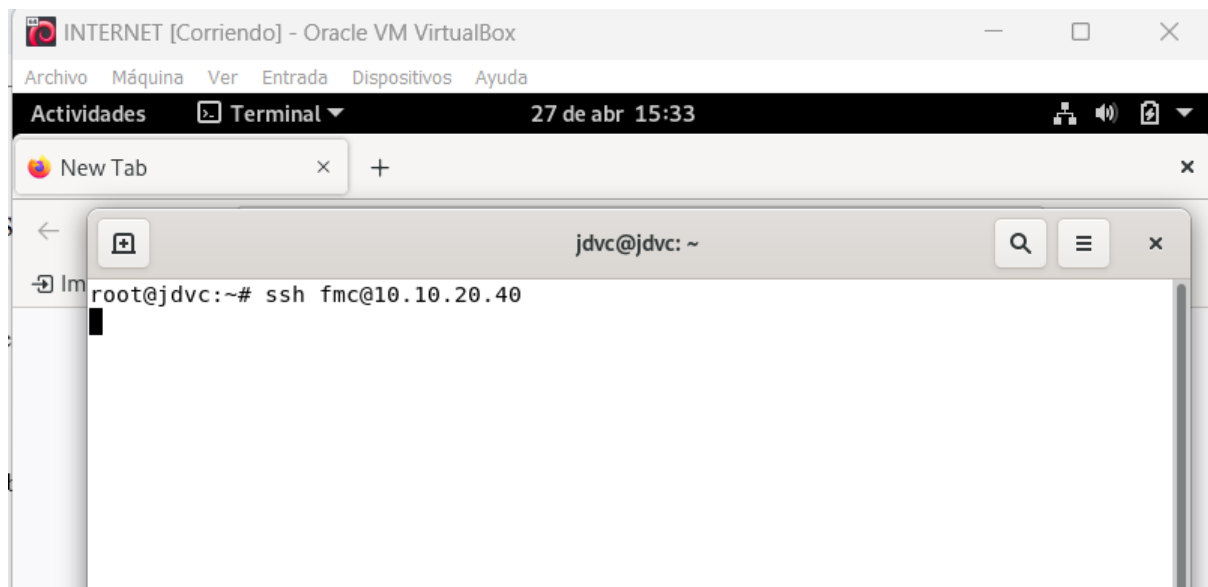
Conexión SSH antes de la configuración de bloqueo del firewall entre Internet y Intranet



### Configuración de Firewall para el bloqueo

```
root@debian:~# iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j DROP
```

## Bloqueo de conexión ssh de Internet a Intranet



## SSH de Internet a DMZ, DB y Web

```
root@internet:/home/servidorweb# ssh vboxuser@10.10.10.50
vboxuser@10.10.10.50's password:
Linux Linux 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Apr 27 12:29:54 2023 from 10.10.20.40
vboxuser@Linux:~$ exit
logout
Connection to 10.10.10.50 closed.
root@internet:/home/servidorweb# ssh vboxuser@10.10.10.80
The authenticity of host '10.10.10.80 (10.10.10.80)' can't be established.
ECDSA key fingerprint is SHA256:5WPzWPe812p1SAIXg7h7hDnCut8r0fAcMYEF0b6anuw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.80' (ECDSA) to the list of known hosts.
vboxuser@10.10.10.80's password:
Linux Linux 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64
```

## SSH de Intranet a DMZ, DB y Web

```
root@debian:~# ssh vboxuser@10.10.10.50
vboxuser@10.10.10.50's password:
Linux Linux 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Apr 27 12:32:51 2023 from 10.10.20.40
vboxuser@Linux:~$ exit
logout
Connection to 10.10.10.50 closed.
root@debian:~# ssh vboxuser@10.10.10.80
vboxuser@10.10.10.80's password:
Linux Linux 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Apr 27 12:24:01 2023 from 10.10.10.50
vboxuser@Linux:~$ █
```

## CONCLUSIÓN

En conclusión, un firewall es una herramienta de seguridad esencial que se utiliza para proteger las redes y los sistemas de posibles amenazas externas. Un firewall funciona al filtrar el tráfico de red y permitir solo el tráfico autorizado, bloqueando todo lo demás. Los firewalls pueden ser software o hardware y se pueden configurar para satisfacer las necesidades específicas de una organización.

Sin embargo, es importante tener en cuenta que los firewalls no son una solución completa de seguridad en sí mismos. Los firewalls son solo una pieza de un enfoque de seguridad más amplio que incluye otras medidas de seguridad como la autenticación, el cifrado y la gestión de parches. Además, los firewalls no pueden proteger contra todas las amenazas, como el malware que se transmite a través de medios extraíbles o el phishing.

En resumen, los firewalls son una herramienta esencial de seguridad, pero deben ser utilizados en conjunto con otras medidas de seguridad para una protección completa y efectiva de los sistemas y redes.



## REFERENCIAS BIBLIOGRÁFICAS

*Configuración de SSH en Linux*. (s. f.). Recuperado 27 de abril de 2023, de

[https://www2.microstrategy.com/producthelp/Current/InstallConfig/es-es/Content/topology\\_config\\_SSH\\_linux.htm](https://www2.microstrategy.com/producthelp/Current/InstallConfig/es-es/Content/topology_config_SSH_linux.htm)

*Crear una base de datos en MySQL / MariaDB*. (s. f.). Styde.net. Recuperado 27 de abril

de 2023, de <https://styde.net/crear-una-base-de-datos-en-mysql-mariadb/>

Cuesta, D. G. (2019, noviembre 12). ▷ Cómo configurar un servidor web Apache »

Linux en español. *Linux en español*.

<https://www.xn--linuxenespaol-skb.com/tutoriales/configurar-servidor-web-apache/>

*Qué es el Internet*. (s. f.). Significados. Recuperado 27 de abril de 2023, de

<https://www.significados.com/internet/>

*¿Qué es un firewall? - Soporte técnico de Microsoft*. (s. f.). Recuperado 27 de abril de

2023, de

<https://support.microsoft.com/es-es/office/-qu%C3%A9-es-un-firewall-6870c88d-69b6-4db4-9cb1-0e4afa7a8603>

*¿Qué es una DMZ y por qué la usaría?* (s. f.). Fortinet. Recuperado 27 de abril de 2023,

de <https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz.html>

*¿Qué es una Intranet?* (s. f.). Recuperado 27 de abril de 2023, de

<https://www.innovaportal.com/innovaportal/v/75/1/innova.front/que-es-una-intranet>